Industry Recognized Credential Transfer Assurance Guide: Information Technology – Security+

CompTIA Security+

April 13, 2022

Industry Recognized Credential Transfer Assurance Guides (ITAGs) are a statewide transfer initiative that guarantees the award of college-level credit to students earning agreed-upon, industry recognized credentials. Students meeting credentialing requirements, regardless of where the learning was achieved, will be eligible to earn credit for specified courses deemed equivalent to the stated industry recognized credential listed on the ITAG document. Credentials are reviewed and aligned to postsecondary learning outcomes that are endorsed by Ohio's public institutions of higher education. The receiving institution must offer an equivalent course or program. Additional information on accessing and awarding ITAG credit is outlined in this document.

Required Credential(s)

Credential Name: CompTIA Security+

Credential Issuer: CompTIA

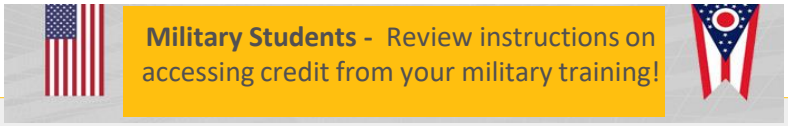
Exam(s): SY0-601

Additional Requirements for Credit: Students must access credit within three years of passing the exam.

Credit Access and Verification

Student: Students wishing to receive credit should create a transcript of their certification via the CompTIA website and email it to the address provided by the institution. https://help.comptia.org/hc/en-us/articles/115005395083-Create-a-Transcript?tracking=help/certificates-credentials-transcripts/credentials/create-a-transcript

Institution: Provide email address for receipt of transcript to student.



Course Information

Course Name: ITITS 015 Information Technology Security (CompTIA Security+)

Credit Hours: 3

Course Description: A current overview of both network and Internet based security practices and conventions; including planning, implementing, and managing network security. Through an exploration of security technologies, vulnerability assessment and attack methods this course offers methods to minimize potential security risks by means of organizational policy, education and technology.

Learning Outcomes and Credential Alignment

Proposed Alignment of CompTIA Security+ Exam Objectives to Postsecondary Learning Outcomes

Postsecondary Learning Outcomes *(Copy of CTIT015)*	**Content from Credential** *(Numbers refer to CompTIA Content Numbering System)*
1. Implement practices to properly harden operating systems and application software on a continuing basis.	2.3 Summarize secure application development, deployment, and automation concepts. 3.1 Given a scenario, implement secure protocols 3.2 Given a scenario, implement host or application security solutions. 3.4 Given a scenario, install and configure wireless security settings. 3.5 Given a scenario, implement secure mobile solutions. 5.1 Compare and contrast various types of controls.
2. Identify commonly used ports and protocols, in both wired and wireless communications, their vulnerabilities and methods to mitigate those vulnerabilities.	3.1 Given a scenario, implement secure protocols 3.3 Given a scenario, implement secure network designs. 3.4 Given a scenario, install and configure wireless security settings. 3.5 Given a scenario, implement secure mobile solutions.
3. Identify and implement software and hardware tools (IP scanning, packet sniffing, and others) to increase network security.	3.3 Given a scenario, implement secure network designs. 2.7 Explain the importance of physical security controls. 2.6 Explain the security implications of embedded and specialized systems.
4. Conduct risk and vulnerability assessments and implement appropriate plans to mitigate common risks and vulnerabilities.	1.1 Compare and contrast different types of social engineering techniques. 1.2 Given a scenario, analyze potential indicators to determine the type of attack. 1.3 Given a scenario, analyze potential indicators associated with application attacks. 1.4 Given a scenario, analyze potential indicators associated with network attacks. 1.5 Explain different threat actors, vectors, and intelligence sources 1.6 Explain the security concerns associated with various types of vulnerabilities. 1.7 Summarize the techniques used in security assessments. 1.8 Explain the techniques used in penetration testing.

Learning Outcomes and Credential Alignment *(cont.)*

5. Implement procedures to properly log system events, review those logs and audit security settings on a regular basis.	4.5 Explain the key aspects of digital forensics.
6. Explain and implement redundancy planning, disaster recovery and incident response as means to provide business continuity.	2.5 Given a scenario, implement cybersecurity resilience 4.3 Given an incident, utilize appropriate data sources to support an investigation. 4.4 Given an incident, apply mitigation techniques or controls to secure an environment. 5.4 Summarize risk management processes and concepts.
7. Explain the impact of organizational policy, state and federal legislation, and environmental controls on security planning.	2.1 Explain the importance of security concepts in an enterprise environment. 4.1 Given a scenario, use the appropriate tool to assess organizational security 4.2 Summarize the importance of policies, processes, and procedures for incident response. 5.1 Compare and contrast various types of controls. 5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture. 5.3 Explain the importance of policies to organizational security. 5.5 Explain privacy and sensitive data concepts in relation to security
8. Compare and contrast access control methods including role based, discretionary, mandatory and rule based and implement appropriately to secure network resources.	2.4 Summarize authentication and authorization design concepts. 3.7 Given a scenario, implement identity and account management controls.
9. Summarize and deploy various authentication methods including password based, biometric and certificate-based models.	2.4 Summarize authentication and authorization design concepts. 3.7 Given a scenario, implement identity and account management controls. 3.8 Given a scenario, implement authentication and authorization solutions.

Learning Outcomes and Credential Alignment *(cont.)*

10. Explain general cryptographic concepts including hashing, symmetric and asymmetric encryption, digital certificates and public key infrastructure (PKI).	2.8 Summarize the basics of cryptographic concepts. 3.9 Given a scenario, implement public key infrastructure.
11. Explain secure protocols including Secure Socket Layer (SSL) and IPSec to provide encrypted communication.	3.3 Given a scenario, implement secure network designs.
12. Summarize and apply Virtualization and Cloud concepts .	2.2 Summarize virtualization and cloud computing concepts 3.6 Given a scenario, apply cybersecurity solutions to the cloud.

ITAG Development Panel

Name	Institution/Organization	Role
Ryan Moore	University of Cincinnati	Lead Panel Member - Faculty
Kyle Jones	Sinclair Community College	Panel Member – Faculty
Ryan Burgess	Warren County Career Center	Panel Member – OTC Representative
Thomas O'Neill	Butler Tech	Panel Member – Secondary Representative
Dr. Carl Brun	Ohio Department of Higher Education	ODHE Consultant for ITAGs
Nikki Wearly	Ohio Department of Higher Education	Director, Career-Technical Education Transfer Initiatives